arXiv:1001.2638v2 [math.NT] 16 Apr 2010

Elementary Trigonometric Sums related to Quadratic Residues

A. Laradji* M. Mignotte† N. Tzanakis‡

Let p be an odd prime. We will study the following sums

$$T(p) = \sqrt{p} \sum_{n=1}^{(p-1)/2} \tan \frac{\pi n^2}{p} \tag{1}$$

and

$$C(p) = \sqrt{p} \sum_{n=1}^{(p-1)/2} \cot \frac{\pi n^2}{p}\,. \tag{2}$$

Surprisingly, we came across these sums as we were working on a certain diophantine equation. Being non specialists in the relevant area, we were impressed by the nice properties that these sums have and their elegant consequences. It is this feeling of elegance that we would like to share with our readers. As pointed out to us by Juan Carlos Peral Alonso, to whom we are grateful, these sums are closely related to the *class-number formula* due to Dirichlet (see (19)), sometimes called "Lebesgue's formula" –see [9], p. 179–, which "explains", in a sense, their nice properties. For those readers who are not already acquainted with the notion of *class-number*, a brief remark has its place. Let D be a negative integer which is a *fundamental discriminant*, i.e. either $D \equiv 1 \pmod 4$ and D is squarefree, or $D \equiv 0 \pmod 4$ and $D/4$ is squarefree $\equiv 2, 3 \pmod 4$. In particular, if p is a prime $\equiv 3 \bmod 4$ (we will deal with such primes in this paper), $-p$ is a fundamental discriminant. The *class-number* $h(D)$ has a double interpretation, as the number of reduced binary quadratic forms of discriminant D, and as the number of classes of fractional ideals of the quadratic number field $\mathbb{Q}(\sqrt{D})$. The reader may very well profit by reading, for example, sections 4.9.1, 5.1, 5.2 and 5.3.1 of H. Cohen's book [7], written in a very concrete way; see, especially, the conclusion following Lemma 5.3.4 therein.

All the results presented in this paper, possibly with the exception of Properties 1, 3 and 5, are scattered in the literature, mainly (but not exclusively) in articles about the class-number of binary quadratic forms; see, for example, [9] and [16]. Therefore, our purpose is not to present new results; rather having expository-pedagogic aim, our paper offers a bouquet of classical results which are presented with a very smooth, as we believe, manner, practically using only Elementary Mathematics, or appealing to short and easily readable elementary papers, like [2], [4], [6],[18], [19].

*Department of Mathematics & Statistics, KFUPM, Dhahran, Saudi Arabia, e-mail: alaradji@kfupm.edu.sa

†Université Louis Pasteur,U. F. R. de Mathématiques, Strasbourg, France, e-mail: maurice@math.u-strasbg.fr

‡Department of Mathematics, University of Crete, Iraklion, Greece, e-mail: tzanakis@math.uoc.gr, http://www.math.uoc.gr/~tzanakis

Since $T(p)$ and $C(p)$ are very closely related to each other (see (15)), we will mainly focus on $T(p)$. We also note that our $T(p)$ is equal to H.L. Montgomery's $-T(1,\chi)$ as defined in [17], where χ is the non-trivial quadratic character.

As we will see immediately below, if $p \equiv 1 \pmod 4$, then $T(p) = 0 = C(p)$, therefore, concerning the sums $T(p)$ and $C(p)$, only the case $p \equiv 3 \pmod 4$ is of interest. For this case, we prove a number of elegant number-theoretical properties of $T(p)$. Some of them have the flavour of the well-known property of the primes $p \equiv 3 \pmod 4$, asserting that, in the range 1 to $(p-1)/2$ there are more quadratic residues $\bmod p$ than non-quadratic residues (see, for example, [6], [18], [19]). Further, Properties 1 and 2 below give a simple rule comparing the numbers of even and odd quadratic residues in $\{1, 2, \ldots, p-1\}$ and Property 5 gives an extremely simple rule for expressing $h(-p)$, the class-number of the quadratic field $\mathbb{Q}(\sqrt{-p})$.

First, a few remarks have their place. If Q is any complete set of quadratic residues $\bmod p$, we can write

$$T(p) = \sqrt{p} \sum_{j \in Q} \tan \frac{\pi j}{p}\,.$$

If $p \equiv 1 \pmod 4$, then $-Q \equiv Q \pmod p$, from which we immediately conclude that $T(p) = 0$ and, similarly, $C(p) = 0$. Therefore we make the following assumption:

Throughout this paper, p will always denote a prime $\equiv 3 \pmod 4$.

We denote by ζ a primitive p-root of unity and we put $i = \sqrt{-1}$. Also, by $\sqrt{p}$ we mean the positive square root of p. It is easy to see that

$$T(p) = i\sqrt{p} \sum_{j \in Q} \frac{1-\zeta^j}{1+\zeta^j}\,, \tag{3}$$

therefore, we have

$$\begin{aligned}
T(p) =& i\sqrt{p} \sum_{=1}^{(p-1)/2} \frac{1-\zeta^{j^2}}{1+\zeta^{j^2}} = i\sqrt{p} \sum_{j=1}^{(p-1)/2} \left(\frac{2}{1+\zeta^{j^2}} - 1 \right) = i\sqrt{p} \sum_{j=1}^{(p-1)/2} \left(\frac{1+(\zeta^{j^2})^p}{1+\zeta^{j^2}} - 1 \right) \\
=& i\sqrt{p} \sum_{j=1}^{(p-1)/2} \left(1 - \zeta^{j^2} + (\zeta^{j^2})^2 - \cdots + (\zeta^{j^2})^{p-1} - 1 \right) \\
=& i\sqrt{p} \sum_{j=1}^{(p-1)/2} \left(-\zeta^{j^2} + (\zeta^{j^2})^2 - \cdots + (\zeta^{j^2})^{p-1} \right) \\
=& \frac{i\sqrt{p}}{2} \sum_{j=1}^{p-1} \left(-\zeta^{j^2} + (\zeta^{j^2})^2 - \cdots + (\zeta^{j^2})^{p-1} \right) \\
=& \frac{i\sqrt{p}}{2} \sum_{k=1}^{p-1} (-1)^k \sum_{j=1}^{p-1} \zeta^{j^2 k} = \frac{i\sqrt{p}}{2} \sum_{k=1}^{p-1} (-1)^k \sum_{j=0}^{p-1} \zeta^{j^2 k}\,.
\end{aligned} \tag{4}$$

For every $k = 1, \ldots, p-1$, $\displaystyle\sum_{j=0}^{p-1} \zeta^{j^2 k}$ is the well-known Gaussian sum, denoted by $S(k,p)$, which is equal to $i \left(\frac{k}{p}\right) \sqrt{p}$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. This is a straightforward

consequence of the following more general well-known result:
Let m be an odd positive number and let n be an integer relatively prime to m.
Put $S(k,m) = \sum_{j=0}^{m-1} e^{2\pi i j^2 k/m}$. *Then,*

$$S(n,m) = \begin{cases} \left(\frac{k}{m}\right)\sqrt{m} & \text{if } m \equiv 1 \pmod 4 \\ i\left(\frac{k}{m}\right)\sqrt{m} & \text{if } m \equiv 3 \pmod 4 \end{cases}$$

See, e.g. Theorem 5.6 in Chapter 7 of [13]. When m is a prime $p \equiv 3 \pmod 4$, we can more directly prove that

$$S(k,p) = i\left(\frac{k}{p}\right)\sqrt{p}\,, \tag{5}$$

without appealing to the above result, by turning to a short paper of Bamba and Chowla [2]. In that paper, an interesting brief and elementary proof of the relation $(1-i)(1+i^m)S(1,m) = 2\sqrt{m}$, where m is positive odd integer, is given. Consequently, if p is a prime $\equiv 3 \pmod 4$, then $S(1,p) = i\sqrt{p}$. By the definition of $S(k,m)$ it is clear that, if k is a quadratic residue $\bmod p$, then $S(k,p) = S(1,p)$; and if k is a quadratic non-residue, then

$$S(k,p) = S(-1,p) = \overline{S(1,p)} = \overline{i\sqrt{p}} = -i\sqrt{p}\,,$$

as claimed.
Now, going back to (4) and using (5), we obtain the following expression for $T(p)$:

$$T(p) = \frac{p}{2}\sum_{k=1}^{p-1}(-1)^{k+1}\left(\frac{k}{p}\right)\,. \tag{6}$$

Let $a_1, a_2, \ldots, a_\mu$ and $b_1, b_2, \ldots, b_\nu$ be, respectively, the even and odd quadratic residues $\bmod p$ in the set $P = \{1, 2, \ldots, p-1\}$. Clearly, $\mu+\nu = (p-1)/2$ and the set of the quadratic non-residues $\bmod p$ in P is $\{p-a_1, \ldots p-a_\mu, p-b_1, \ldots, p-b_\nu\}$. Note that a summand $(-1)^{k+1}\left(\frac{k}{p}\right)$ in the right-hand side of (6) is positive iff $k \in \{p-b_1, \ldots, p-b_\nu, b_1, \ldots, b_\nu\}$, i.e. 2ν summands are positive and, analogously, 2μ summands are negative. Then, $T(p) = p(\nu-\mu)$, where we observe that $\nu-\mu$ is and odd number, since $\nu+\mu = (p-1)/2$. Thus, we have the following:

Property 1. *Let p be a prime* $\equiv 3 \pmod 4$ *and let $q_o(p)$ and $q_e(p)$ be, respectively, the number of odd and even quadratic residues* $\bmod p$ *in the set* $\{1, 2, \ldots, p-1\}$. *Then*

$$T(p) = p(q_o(p) - q_e(p))\,. \tag{7}$$

In particular, $T(p)$ is an odd integer divisible by p and by no higher power of p.

Next, we rewrite the definition (1) of $T(p)$ as follows,

$$T(p) = \frac{\sqrt{p}}{2}\sum_{n=1}^{p-1}\tan\frac{n^2\pi}{p}\,. \tag{8}$$

We have the following inequality of A.L. Whiteman (Theorem 2 of [19]):

$$\sum_{n=1}^{p-1}\cot\frac{n^2\pi}{p} > 0\,. \tag{9}$$

In view of the identity $\tan\theta = \cot\theta - 2\cot 2\theta$, the relation (8) becomes

$$\frac{2}{\sqrt{p}}T(p) = \sum_{n=1}^{p-1} \cot\frac{n^2\pi}{p} - 2\sum_{n=1}^{p-1} \cot\frac{2n^2\pi}{p}\,. \tag{10}$$

If $p \equiv 7 \pmod 8$, then the sets $\{2n^2 : n = 1,\dots,p-1\}$ and $\{n^2 : n = 1,\dots,p-1\}$ are identical $\bmod p$, hence, the right-hand side of (10) is equal to $-\sum_{n=1}^{p-1} \cot\frac{n^2\pi}{p}$ and, by Whiteman's inequality (9), it is strictly negative.
If $p \equiv 3 \pmod 8$, then the sets $\{2n^2 : n = 1,\dots,p-1\}$ and $\{-n^2 : n = 1,\dots,p-1\}$ are identical $\bmod p$, because both -2 and -1 are quadratic non-residues. Therefore, the right-hand side of (10) is equal to $3\sum_{n=1}^{p-1} \cot\frac{n^2\pi}{p}$, hence, by (9), it is strictly positive. Thus, in combination also with Property 1, we obtain the following:

Property 2. *$T(p) > 0$ if $p \equiv 3 \pmod 8$ and $T(p) < 0$ if $p \equiv 7 \pmod 8$. Also, in the set $\{1, 2, \dots, p-1\}$, the odd quadratic residues $\bmod p$ are more than the even ones when $p \equiv 3 \pmod 8$; the reverse situation is true when $p \equiv 7 \pmod 8$.*

Now consider the sum

$$M(p) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) k\,.$$

Dirichlet [10] proved that, for $p \equiv 3 \pmod 4$, $M(p) < 0$, i.e. among the numbers $1, 2, \dots, p-1$, the sum of the quadratic non-residues is greater than the sum of the quadratic residues. In [3], B.C. Berndt proves that

$$M(p) = \frac{\sqrt{p}}{2} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \cot\frac{k\pi}{p} \tag{11}$$

and, based on (11), he gives (Theorem 3.1 in [3]) another proof of Dirichlet's inequality

$$M(p) < 0 \quad \text{for } p \equiv 3 \pmod 4. \tag{12}$$

Using (11), it is an easy exercise to check that

$$T(p) = \begin{cases} -M(p) & \text{if } p \equiv 7 \pmod 8 \\ 3M(p) & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

This, combined with Property 2, gives now another proof of (12) which is simpler than that of Theorem 3.1 in [3].

An upper bound for $T(p)$. From (7) we trivially obtain $|T(p)| < p(p-1)/2$. However, we can obtain a much better upper bound as follows.
Let $Q \subseteq \{1, 2, \dots, p-1\}$ be a complete set of quadratic residues $\bmod p$. We have

$$|T(p)| \le \sqrt{p} \sum_{j\in Q} \left|\tan\frac{\pi j}{p}\right| = \sqrt{p} \sum_{j\in Q} \frac{1}{\left|\tan\frac{\pi(p-2j)}{2p}\right|}\,.$$

Since $\left|\frac{\pi(p-2j)}{2p}\right| < \frac{\pi}{2}$, it follows that $\left|\tan\frac{\pi(p-2j)}{2p}\right| > \frac{\pi}{2p}|p-2j|$, hence,

$$|T(p)| < \frac{2p\sqrt{p}}{\pi}\sum_{j\in Q}\frac{1}{|p-2j|}\,.$$

Note that, as j runs through the set Q, the numbers $|p-2j|$ are distinct $\bmod p$, for, if $|p-2j_1| \equiv |p-2j_2| \pmod p$ with $j_1, j_2 \in Q$ and $j_1 \neq j_2$, then, necessarily, $j_2 = -j_1$, which implies that -1 is a quadratic residue $\bmod p$, a contradiction. Therefore, the set $\{|p-2j| : j \in Q\}$ is a subset of $\{1,\dots,p-1\}$ with cardinality $(p-1)/2$, consisting of odd numbers, i. e. it coincides with $\{1,3,\dots,p-2\}$. Therefore,

$$\sum_{j\in Q}\frac{1}{|p-2j|} \leq \sum_{k=1}^{(p-1)/2}\frac{1}{2k-1} < 1+\frac{1}{2}\log(p-2)\,,$$

from which we obtain the following:

Property 3. *For any prime $p \equiv 3 \pmod 4$ we have*

$$|T(p)| < \frac{2p\sqrt{p}}{\pi}(1+\frac{1}{2}\log(p-2))\,. \tag{13}$$

Now we go on to the study of $C(p)$. We use the following alternative expression for $C(p)$ (cf. (3)):

$$C(p) = -i\sqrt{p}\sum_{j\in Q}\frac{1+\zeta^j}{1-\zeta^j}\,, \tag{14}$$

where Q is a complete set of quadratic residues $\bmod p$. It is straightforward to check that $C(3) = 1$, therefore we assume that $p > 3$. By Whiteman's inequality (9), we have $C(p) > 0$. Just before obtaining Property 2, we actually proved that $T(p) = -C(p)$ if $p \equiv 7 \pmod 8$ and $T(p) = 3C(p)$ if $p \equiv 3 \pmod 8$. Therefore,

$$C(p) = \begin{cases} -T(p) & \text{if } p \equiv 7 \pmod 8 \\ \frac{1}{3}T(p) & \text{if } p \equiv 3 \pmod 8 \end{cases}. \tag{15}$$

By Property 1, $C(p) \in \mathbb{Z}$ if $p \equiv 7 \pmod 8$ and $C(p) \in \frac{1}{3}\mathbb{Z}$ if $p \equiv 3 \pmod 8$. Actually, $C(p) \in \mathbb{Z}$ always. We show this as follows.
Let $L = \mathbb{Q}(\zeta)$, the p-th cyclotomic field. Over L we have the following factorization of the p-th cyclotomic polynomial $\Phi_p(x)$

$$\Phi_p(x) = x^{p-1}+\cdots+x+1 = \frac{x^p-1}{x-1} = \prod_{k=1}^{p-1}(x-\zeta^k)\,,$$

from which it follows that $1 = \prod_{k=1}^{p-1}(1+\zeta^k)$, implying that $1+\zeta^k$ is a unit in L. In L we have the ideal factorization $\langle p\rangle = \langle\lambda\rangle^{p-1}$, where λ is a prime element. Since $p = \Phi_p(1) = \prod_{k=1}^{p-1}(1-\zeta^k)$, it follows that, $1-\zeta^k = \lambda\times$ unit for every $k = 1,\dots,p-1$. These observations, in combination with (14), imply that $C(p) = \alpha/\lambda$, where $\alpha \in L$ is an algebraic integer. On the other hand, $C(p)$ is a rational number with denominator 1 or 3. If λ does not divide α (in L), then λ must divide the denominator of $C(p)$ which, as just mentioned, is either 1 or 3, and this is impossible because $p > 3$. Therefore λ divides α, hence $C(p) = \alpha/\lambda$ is an algebraic integer; and as $C(p)$ is a rational number, it follows that $C(p) \in \mathbb{Z}$.

Property 4. *$C(3) = 1$ and, for any prime $p \equiv 3 \pmod 4$, $p > 3$, $C(p)$ is an odd positive integer, divisible by p and by no higher power of p. If $p \equiv 3 \pmod 8$, then $T(p)$ is a multiple of 3, hence, by Property 2, $q_o(p) - q_e(p)$ is a positive multiple of 3.*

The following elegant property relates $T(p)$ with the class-number of the quadratic number field $\mathbb{Q}(\sqrt{-p})$.

Property 5. *Let p be a prime number $\equiv 3 \pmod 4$ and let $h(-p)$ be the class-number of the quadratic number field $\mathbb{Q}(\sqrt{-p})$. Then,*

$$T(p) = \begin{cases} -ph(-p) & \text{if } p \equiv 7 \pmod 8 \\ 3ph(-p) & \text{if } p \equiv 3 \pmod 8 \end{cases} \tag{16}$$

$$C(p) = ph(-p) \tag{17}$$

$$h(-p) = \begin{cases} q_e(p) - q_o(p) & \text{if } p \equiv 7 \pmod 8 \\ \frac{1}{3}(q_o(p) - q_e(p)) & \text{if } p \equiv 3 \pmod 8 \end{cases} \tag{18}$$

Proof. We have

$$h(-p) = \frac{1}{2\sqrt{p}} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \cot \frac{k\pi}{p}\,. \tag{19}$$

This is a consequence of the more general formula, referred to as "Lebesgue's formula" in Dickson's "History" [9], p. 179, due to Dirichlet [11]. For a recent proof of that formula we refer the reader to the Corollary 2.3 of [5].
A complete set of quadratic non-residues mod$p$ is $\{-k^2 : k = 1, \ldots, (p-1)/2\}$. Therefore, (19) becomes

$$\begin{aligned} h(-p) &= \frac{1}{2\sqrt{p}}\Big(\sum_{k=1}^{(p-1)/2} \cot \frac{k^2\pi}{p} - \sum_{k=1}^{(p-1)/2} \cot \frac{-k^2\pi}{p}\Big) \\ &= \frac{1}{\sqrt{p}} \sum_{k=1}^{(p-1)/2} \cot \frac{k^2\pi}{p} = \frac{1}{p} C(p)\,, \end{aligned}$$

and now (16), (17) and (18) are straightforward consequencew of (15) and Property 1, respectively. □
The relation (16) is a special case of Corollary 5.2 in [5] which goes back to V.A. Lebesgue [14]. The relation (17) is due to Dirichlet [11]; see also Corollary 3.6 of [5].
Note that, since $q_e(p) + q_o(p) = (p-1)/2$, which is odd, Property 5 implies the following:

For a prime $p \equiv 3 \pmod 4$, $h(-p)$ is odd.

This is Corollary 3.6 of [3].

Further expressions for $T(p)$ and consequences. Since $\left(\frac{p-k}{p}\right) = -\left(\frac{k}{p}\right)$, we have from (6),

$$T(p) = p \sum_{k=1}^{(p-1)/2} (-1)^{k+1} \left(\frac{k}{p}\right)\,. \tag{20}$$

We have

$$\sum_{k=1}^{p-1}(-1)^{k+1}\left(\frac{k}{p}\right) = \left(\frac{1}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-2}{p}\right)-\left(\frac{2}{p}\right)-\left(\frac{4}{p}\right)-\cdots-\left(\frac{p-1}{p}\right) \quad (21)$$

$$= \left(\frac{1}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-2}{p}\right)+\left(\frac{p-2}{p}\right)+\left(\frac{p-4}{p}\right)+\cdots+\left(\frac{1}{p}\right)$$

$$= 2\left(\left(\frac{1}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-2}{p}\right)\right) = 2A\,, \quad (22)$$

where $A = \left(\frac{1}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-2}{p}\right)$. Therefore, by (22) and (21),

$$2A = A - \left(\frac{2}{p}\right)\left(\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots\left(\frac{(p-1)/2}{p}\right)\right),$$

implying

$$A = -\left(\frac{2}{p}\right)\left(\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots\left(\frac{(p-1)/2}{p}\right)\right).$$

Collecting together the expressions for $T(p)$ in (6), (20), (22) and the expression for A just above, we have:

$$T(p) = \frac{p}{2}\sum_{k=1}^{p-1}(-1)^{k+1}\left(\frac{k}{p}\right) \quad (23)$$

$$= p\sum_{k=1}^{(p-1)/2}(-1)^{k+1}\left(\frac{k}{p}\right) \quad (24)$$

$$= 2p\left(\left(\frac{1}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-2}{p}\right)\right) \quad (25)$$

$$= -p\left(\frac{2}{p}\right)\left(\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots\left(\frac{(p-1)/2}{p}\right)\right). \quad (26)$$

Note that the sum appearing in (26) is a sum of the values of a primitive character mod p, therefore, by the Pólya inequality[1] (see Theorem 8.21 in [1] or inequality (2) in Chapter 23 of [8]) this sum is $< p^{1/2}\log p$. This gives the upper bound $|T(p)| < p^{3/2}\log p$, which is slightly worse than the upper bound in Property 3.

The expression (26) for $T(p)$, in combination with a well-known result of Dirichlet saying that, among the numbers $1, 2, \ldots, (p-1)/2$ there are more quadratic residues than non-quadratic residues mod p (see e.g. [6], [19], [18], or exercises 14 through 17, Chapter 16 of [12]) furnishes another proof of Property 2.
Next, equating the right-hand sides of (24) and (26) and separating the Legendre symbols with even "numerators" from those with odd ones, we find

$$\left(1+\left(\frac{2}{p}\right)\right)\left(\left(\frac{1}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{(p-1)/2}{p}\right)\right)$$

$$= \left(1-\left(\frac{2}{p}\right)\right)\left(\left(\frac{2}{p}\right)+\left(\frac{4}{p}\right)+\cdots+\left(\frac{(p-3)/2}{p}\right)\right). \quad (27)$$

[1] Or Pólya-Vinogradov inequality.

If $p \equiv 3 \pmod 8$, then (27) implies that $\left(\frac{2}{p}\right) + \left(\frac{4}{p}\right) + \cdots + \left(\frac{(p-3)/2}{p}\right) = 0$, hence, $\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{(p-3)/4}{p}\right) = 0$, which says that, among the numbers $1, 2, \ldots, (p-3)/4$ there are as many quadratic residues as quadratic non-residues mod p; and since $T(p) > 0$, (26) implies that there are more quadratic residues than quadratic non-residues among the numbers $(p+1)/4, \ldots, (p-1)/2$.
If $p \equiv 7 \pmod 8$, then (27) implies that $\left(\frac{1}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{(p-1)/2}{p}\right) = 0$, hence, $\left(\frac{p-1}{p}\right) + \left(\frac{p-3}{p}\right) + \cdots + \left(\frac{(p+1)/2}{p}\right) = 0$ and, consequently, $\left(\frac{(p+1)/4}{p}\right) + \cdots + \left(\frac{(p-3)/2}{p}\right) + \left(\frac{(p-1)/2}{p}\right) = 0$. This shows that there are as many quadratic residues as quadratic non-residues mod p among the numbers $(p+1)/4, \ldots, (p-1)/2$; and since $T(p) < 0$, (26) implies that there are more quadratic residues than quadratic non-residues among the numbers $1, \ldots, (p-3)/4$.

Property 6. *If $p \equiv 3 \pmod 8$ then, among the numbers $1, 2, \ldots, (p-3)/4$, there are as many quadratic residues as quadratic non-residues* mod p *and among the numbers $(p+1)/4, \ldots, (p-1)/2$ the quadratic residues are more than the quadratic non-residues.*
If $p \equiv 7 \pmod 8$ then, among the numbers $1, 2, \ldots, (p-3)/4$, there are more quadratic non-residues than quadratic residues mod p *and among the numbers $(p+1)/4, \ldots, (p-1)/2$ the quadratic residues are as many as the quadratic non-residues.*
In other words,

$$\sum_{k=1}^{(p-3)/4} \left(\frac{k}{p}\right) \quad \begin{cases} > 0 & \text{if } p \equiv 7 \pmod 8 \\ = 0 & \text{if } p \equiv 3 \pmod 8 \end{cases} \tag{28}$$

$$\sum_{k=(p+1)/4}^{(p-1)/2} \left(\frac{k}{p}\right) \quad \begin{cases} = 0 & \text{if } p \equiv 7 \pmod 8 \\ > 0 & \text{if } p \equiv 3 \pmod 8 \end{cases} \tag{29}$$

The relations (28) and (29) can also be inferred by an argument of B.C. Berndt and S. Chowla (p. 8 of [4]) in combination of their main Theorem therein, applied with $q = 2$.

Property 6 implies another interesting fact, already noted in 1979, namely,

Property 7. *If $p \equiv 3 \pmod 8$, then the number of even quadratic residues* mod p *that are $< p/2$ equals $(p-3)/8$. If $p \equiv 7 \pmod 8$, then the number of even quadratic residues that are $> p/2$ equals $(p+1)/8$.*

The fact that Property 7 is implied by Property 6 is noted by Emma Lehmer [15].
Finally, we remark that our arguments that led to Property 6 furnish another expression for $T(p)$, namely,

$$T(p) = \begin{cases} p\left(\left(\frac{(p+1)/4}{p}\right) + \cdots + \left(\frac{(p-3)/2}{p}\right) + \left(\frac{(p-1)/2}{p}\right)\right) & \text{if } p \equiv 3 \pmod 8 \\ p\left(\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) \cdots + \left(\frac{(p-3)/4}{p}\right)\right) & \text{if } p \equiv 7 \pmod 8 \end{cases} \tag{30}$$

References

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York 1976.

[2] R.P. Bambah, S. Chowla, On the sign of the Gaussian sum, *Proc. Nat. Inst. Sci. India* **13** (1947), 175-176.

[3] B.C. Berndt, Classical theorems on quadratic residues, *Enseign. Math.* **22** (1976), 261-304.

[4] B.C. Berndt, S. Chowla, Zero sums of the Legendre symbol, *Nordisk Mat. Tidskrift* **22** (1974), 5-8.

[5] B.C. Berndt, A. Zaharescu, Finite trigonometric sums and class numbers, *Math. Ann.* **330** (2004), 551-575.

[6] Kai-Lai Chung, Note on a theorem on quadratic residues, *Bull. Am. Math. Soc.* **47** (1941), 514-516.

[7] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer Graduate Texts in Mathematics No 138, Berlin Heidelberg 1993.

[8] H. Davenport, *Multiplicative Number Theory - Second Edition*, Graduate Texts in Mathematics Vol. 74, Springer-Verlag, New York 1980.

[9] L.E. Dickson, *History of the Theory of Numbers*, Vol. III, Chelsea Publishing Co., New York 1971.

[10] G.L. Dirichlet, Recherches sur diverses applications de l' analyse infinitésimale à la théorie des nombres, *Reine Angew. Math.* **19** (1839), 324-369.

[11] G.L. Dirichlet, Recherches sur diverses applications de l' analyse infinitésimale à la théorie des nombres, seconde partie, *J. Reine Angew. Math.* **21** (1840), 134-155.

[12] K. Ireland, M. Rosen, *A classical introduction to modern Number Theory*, Graduate Texts in Mathematics Vol. 84, Springer-Verlag, New York 1982.

[13] Hua Loo Keng, *Introduction to Number Theory*, Springer Verlag, Berlin 1982.

[14] V.A. Lebesgue, Suite du Memoire sur les applications du symbole $\left(\frac{a}{b}\right)$, *J. de Math.* **15** (1850), 215-237.

[15] E. Lehmer, Solution of Problem 6156, *Am. Math. Monthly* **86** No 2 (1979), 134-135.

[16] M. Lerch, Essais sur le calcul de nombre des classes de formes quadratiques binaires aux coefficients entiers, *Acta Math.* **29** (1905), 333-424; *Acta Math.* **30** (1906), 203-293.

[17] H.L. Montgomery, An exponential polynomial formed with the Legendre symbol, *Acta Arith.* **37** (1980), 375-380.

[18] L. Moser, A theorem on quadratic residues, *Proc. Am. Math. Soc.* **2** No 3 (1951), 503-504.

[19] A.L. Whiteman, Theorems on quadratic residues, *Mathematics Magazine* **23** No 2 (1949), 71-74.